제18회 한국정보처리학회 추계학술발표대회 논문집 제9권 제2호 (2002.11)

공중 무선랜에서의 무선 서비스 사업자간 로밍 메커니즘

임수철, 김태윤
고려대학교 컴퓨터학과
e-mail:causal@netlab.korea.ac.kr

A Roaming Mechanism between Wireless Internet Service Providers of Public Wireless LAN

Soo-Chul Lim*, Tai-Yun Kim*
*Dept. of Computer Science and Engineering, Korea University

요 약

본 논문에서는 공중 무선랜에서 AP의 중복 설치로 인해 과열 투자와 주파수 간섭 현상의 문제를 해결하기 위해 무선랜 사업자간(WISP, Wireless Internet Service Provider)의 로밍을 제공할 수 있는 메커니즘을 제안한다. 제안하는 메커니즘은 무선랜 사용자가 자신의 WISP가 아닌 다른 WISP의 AP에서 인터넷에 접속하려 할 때 EAP-TLS(Extended Authentication Protocol - Transport Layer Security)를 인증방법으로 사용하는 것을 전제한다. EAP-TLS를 사용하여 상호 인증과 키 분배를 할 때 필요되는 인증서를 방문한 WISP에게 임시 사용자 인증서를 발급받는 방법으로 로밍을 수행한다.

1. 서론

1990년대 초반부터 제품이 출시된 무선랜은 유선랜에 비해 느린 전송속도와 높은 가격 등의 이유로 인해 널리 사용되지 못하였다. 그러나 IEEE 802.11 Work Group이 11Mbps의 전송율을 제공할 수 있는 IEEE 802.11b의 표준화를 완료함에 따라 전송율과 가격 문제를 해결하게 되었다. 이로 인해 무선랜 시장은 빠른 성장을 보이기 시작하였다.

현재 무선랜 시장은 학교나 회사와 같은 장소뿐만이 아닌 공공으로 사용되는 호텔, 공항, 병원, 카페 등 이용자가 밀집되어 있는 Hot Spot 지역에서 무선랜 기술을 이용하여 서비스를 제공한다.

공중 무선랜 서비스의 활성화를 위해서는 보다 많은 서비스 영역 확보가 필요하며, 이를 위해 사업자간 연동이 필수적이다. 하나의 AP(Access Point)가 서비스할 수 있는 셀 반경은 70-100m에 불과하므로 일정정도의 서비스 영역 확보를 위해서는 많은 수의 AP 설치가 필요하다. 하지만 대부분의 각 사업자들이 서비스하려는 Hot Spot들은 중복되어, 무선랜 서비스 영역 확보를 위한 과열 중복 투자가 발생할 가능성이 높다. 또한 중복 설치로 인해 동일 채널 주파수를 2개 사업자 이상이 사용할 경우, 상호 간섭이 일어나고 인터넷 접속 속도 저하등의 현상이 발생할 수 있다. 따라서 중복 설치를 방지하거나 사업자간 로밍을 제공해야 한다[1].

본 논문에서는 AP의 중복 설치로 인해 과열 투자와 주파수 간섭 현상의 문제를 해결하기 위해 무선랜 사업자간(WISP, Wireless Internet Service Provider)의 로밍을 제공할 수 있는 메커니즘을 제안한다. 제안하는 메커니즘은 무선랜 사용자가 자신의 WISP가 아닌 다른 WISP의 AP에서 인터넷에 접속하려 할 때 EAP-TLS(Extended Authentication Protocol - Transport Layer Security)[2]를 인증방법으로 사용하는 것을 전제한다. EAP-TLS를 사용하여 상호 인증과 키 분배를 할 때 필요되는 인증서를 방문한 WISP에게 임시 사용자 인증서를 발급받는 방법으로 로밍을 수행한다.

본 논문의 구성은 다음과 같다. 2장에서는 WISP간의 로밍을 제공하기 위해 제안된 인증서 분배 구조와 임시 사용자 인증서를 기술한다. 3장에서는 임시 사용자 인증서를 사용하여 WISP간의 로밍을 지원하는 메커니즘을 제안하고, 4장에서는 임시 사용

자 인증서 분배 프로토콜의 분석을 한다. 마지막으로 5장에서는 결론과 향후 연구 과제를 기술한다.

2. 관련 연구

본 장에서는 WISP간의 로밍을 위해 VeriSign에서 제안한 인증서 분배 구조[6]와 [3]에서 제안한 임시 사용자 인증서를 기술한다.

2.1 임시 사용자 인증서

[3]에서 제안한 임시 사용자 인증서는 ASPeCT의 AIP(Authentication and Initialization of Payment) [4] 프로토콜에서 이동 사용자가 외부 도메인의 서비스 제공자에 인증서를 검증할 수 있는 공개키를 보다 효율적으로 공유할 수 있도록 한 것이다. 임시 사용자 인증서 발급은 다음과 같은 단계로 이루어진다.

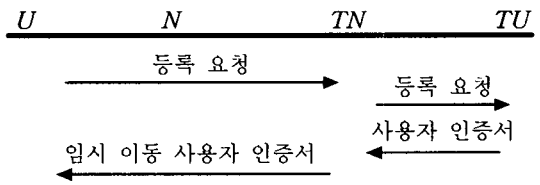

그림 1. 임시 사용자 인증서 발급 프로토콜 모델

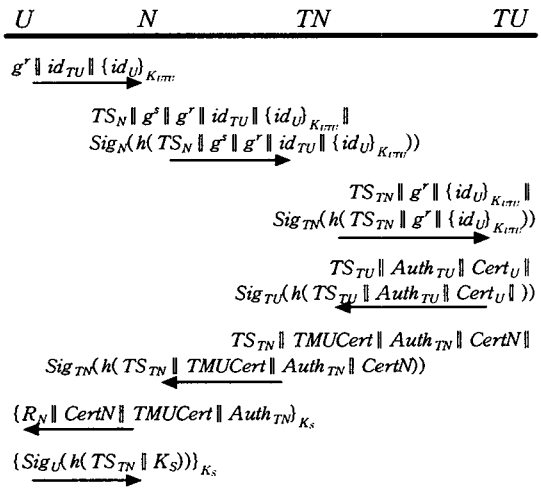

그림 2. 임시 이동 사용자 인증서 발급 프로토콜

그림 1에서 U는 사용자, N은 네트워크 운영자, TN은 네트워크 운영자의 신뢰기관, TU는 사용자의 신뢰기관이다.

그림 2의 프로토콜을 수행한 후, U는 TN이 발급한 임시 사용자 인증서를 사용하여 N의 도메인에서 서비스를 받을 수 있다.

2.2 VeriSign의 로밍 시스템 구조

VeriSign의 로밍을 위한 시스템 구조는 공개키 기반 인증방법(EAP-TLS, EAP-AKA, etc)을 사용하는 무선랜에서 로밍을 지원하기 위해 제안하였다. 공개키 기반 인증방법으로 무선랜 사용자가 인터넷에 접속하려 할 때 사용자는 자신의 WISP가 발행한 인증서를 다른 WISP에서도 사용할 수 있어야만 WISP간의 로밍이 가능하다. VeriSign에서는 그림 3과 같이 인증서를 WISP간에 사용할 수 있도록 하였다.

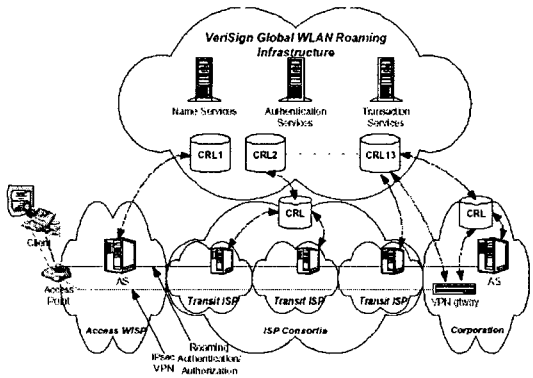

그림 3. WISP간의 VeriSign 로밍 시스템 구조

그림 3에서 사용자가 자신이 가입한 WISP가 아닌 다른 WISP의 AP를 통하여 인터넷 서비스를 받기 위해서는 자신의 WISP에게 인증 확인을 받아야 한다. 또한 사용자가 다른 WISP에서 서비스를 받은 후 서비스 종료를 행하기 전에 사용자의 WISP에게 알린다.

VeriSign의 로밍 시스템 구조는 인증서를 WISP간의 로밍에서 사용할 수 있도록 인증서 분배 및 폐지를 위해 제안된 시스템 구조이다.

3. 제안한 로밍 메커니즘

VeriSign의 로밍을 위한 시스템 구조는 WISP간에 안전하게 로밍을 수행할 수 있도록 신뢰할 수 있는 인증 하부 구조를 제안하였다. 그러나 안전한 하부 구조만을 제안하였을 뿐 실질적인 인증서 발급이나 폐지에 관한 메커니즘은 제안하지 않았다. 본 장에서는 802.1x의 EAP-TLS 인증방법을 사용할 때

WISP간 로밍을 수행할 수 있는 메커니즘을 제안한다.

WISP간 로밍을 수행하기 위한 임시 사용자 인증서(TUCert)를 발급받는 과정은 그림 4와 같다.

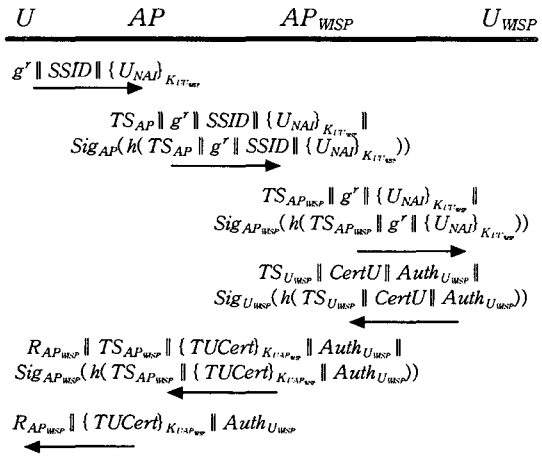

그림 4. 임시 사용자 인증서 분배 프로토콜

그림 4의 임시 사용자 인증서 분배 프로토콜은 U는 무선랜 사용자이고 AP는 U가 인터넷 서비스를 받으려고 하는 Access Point, AP_{WISP}는 AP의 WISP AAA(WISP Authentication, Authorization, Accounting) 서버, U_{WISP}는 U의 WISP AAA 서버로 구성된다. 임시 사용자 인증서 분배 프로토콜은 U가 난수 r을 생성하고 임시 공개 키 설정 키 g^r을 계산해 낸다. U_{WISP}의 신원인 SSID와 U_{WISP}와의 세션키인 $K_{U\,U_{WISP}}$로 암호화한 U의 신원을 - NAI(Network Access Identifier)[5]로 구성 (예, aaa@korea.ac.kr) - AP에게 전송한다. U의 신원을 암호화한 이유는 U의 익명성 보장과 U_{WISP}가 세션키를 통해 U의 개체 인즈을 제공하기 위해서이다. U_{WISP}와의 세션키는 다음과 같이 계산한다.

$$K_{U\,U_{WISP}} = (g^{uw})^r$$

여기서 g^{uw}는 U_{WISP}의 공개키이다.

첫 번째 메시지를 받은 AP는 U에게 받은 메시지와 자신이 생성한 타임스템프 TS_{AP}를 전자 서명하여 AP_{WISP}에게 전송한다.

AP_{WISP}는 AP의 전자 서명을 확인한 후 자신의 타임스템프 $TS_{AP_{WISP}}$와 U의 임시 공개키, 암호화된 U의 신원를 전자 서명하여 U_{WISP}에게 전송한다.

AP_{WISP}에게 메시지를 전송받은 후 U_{WISP}는 g^r과 자신의 비밀키를 사용하여 $(g^r)^{uw}$ 세션키를 생성한다. 이를 사용하여 U의 신원을 확인하고, 올바른 사용자이면 AP_{WISP}에게 $TUCert$를 발급하도록 $CertU$를 전송한다. 이때 U가 AP_{WISP}를 신뢰할 수 있도록 $Auth_{U_{WISP}}$를 같이 전송한다. $Auth_{U_{WISP}}$는 AP_{WISP}의 공개키 g^{apw}와 신원을 포함하고 있으며 다음과 같이 구성된다..

$$Auth_{U_{WISP}} = \left\{ Sig_{U_{WISP}}(h(g^{apw} \,\|\, id_{AP_{WISP}}) \,\|\, g^{apw} \,\|\, id_{AP_{WISP}} \right\}_{K_{U\,U_{WISP}}}$$

AP_{WISP}는 전자 서명을 확인한 후에 $TUCert$를 생성한다. $TUCert$는 발행자와 사용자, 사용자의 공개키, 사용기간이 포함되어 있다. 또한 U와의 세션키를 생성하여 $TUCert$를 암호화한다. 세션키는 다음과 같다.

$$K_{U\,AP_{WISP}} = h((g^r)^{apw} \,\|\, R_{AP_{WISP}})$$

여기서 $R_{AP_{WISP}}$는 AP_{WISP}가 생성한 난수이다.

AP는 AP_{WISP}에게 받은 메시지를 전자 서명 확인을 한 후에 U에게 메시지를 전송한다.

U는 U_{WISP}와의 세션키를 사용하여 복호화를 수행하여 AP_{WISP}의 신원과 공개키를 확인하고, 공개키를 사용하여 전자 서명을 확인한다. 또한 AP_{WISP}의 공개키와 난수를 사용하여 AP_{WISP}와의 세션키를 생성한 후 복호화하여 임시 사용자 인증서인 $TUCert$를 획득할 수 있다.

임시 사용자 인증서는 그림 5와 같이 EAP-TLS를 수행하기 전에 발급받는다. 사용자 U는 AP_{WISP}가 보내는 EAP_Request type EAP-TLS를 받은 후 로밍을 수행하기 위한 Roaming Request 메시지를 전송하여 WISP간의 로밍을 수행한다는 사실을 AP에게 알린다. Roaming Request를 전송받은 AP_{WISP}의 AAA 서버는 $TUCert$를 발급하기 위한 과정을 진행한다. 그림 5와 같이 임시 사용자 인증서 $TUCert$를 획득한 U는 AP_{WISP}의 AAA 서버와 EAP-TLS 인증 방법을 사용하여 상호 인증 및

키 분배를 수행한다. 이를 수행함으로써 사용자는 AP를 통하여 인터넷 서비스를 받을 수 있게된다.

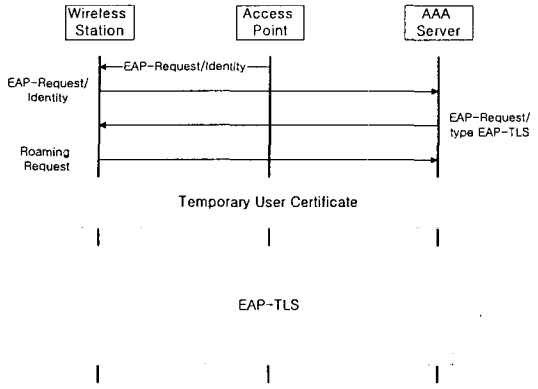

그림 5. WISP간의 로밍을 지원하는 EAP-TLS 메커니즘

4. 안전성 분석

본 논문에서 제안한 WISP간의 로밍 메커니즘은 EAP-TLS 인증 방법을 사용하기 전에 사용자가 방문한 WISP에서 사용할 수 있는 임시 사용자 인증서를 발급받은 후에 이를 사용하여 EAP-TLS 인증 방법으로 상호 인증 및 키 분배를 수행한다. 이 메커니즘이 안전하게 수행하기 위해서는 임시 사용자 인증서 발급 프로토콜이 안전하게 수행되어야 한다. 임시 사용자 인증서 발급 프로토콜은 다음과 같은 안전성을 만족시킨다.

- U와 U_{WISP}간의 상호 인증 : U와 U_{WISP}와의 세션키를 사용하여 U_{NAI}를 암·복호화를 하는 것으로 제공.
- U_{WISP}에 대한 키 인증과 확인 : U_{WISP}가 $Auth_{U_{WISP}}$의 메시지를 세션키로 암호화하는 것으로 제공.
- U와 AP_{WISP}간의 상호 인증 : U_{WISP}가 $Auth_{U_{WISP}}$의 메시지에 AP_{WISP}의 신원과 공개키를 서명하는 것으로 U는 AP_{WISP}를 인증하며, AP_{WISP}는 U_{WISP}에게 $CertU$를 받는 것으로 U를 인증한다.
- AP_{WISP}에 대한 키 인증과 확인 : $TUCert$를 U와의 세션키로 암호화하는 것으로 제공.
- 새로운 키 제공 : $TUCert$를 분배받는 과정에서의 모든 세션키는 사용자가 생성한 난수 r을 포함한다. 이는 세션키가 재 사용되는 것과 새로운 키(key freshness)임을 증명한다.

5. 결론 및 향후 연구 과제

본 논문에서는 공개키 기반의 무선랜 인증 방법을 사용할 때 사용자가 위치해 있는 WISP의 AAA 서버를 통해서 임시 사용자 인증서를 발급받는 방법을 통해 공중 무선랜 서비스 제공자간의 로밍 메커니즘을 제안하였다. 802.1x의 EAP-TLS를 사용하여 인증을 수행할 때 로밍을 위해 임시 사용자 인증서 발급으로 인한 통신량이 증가한다는 문제점을 가지고 있으나, 이는 무선랜 단말기에 크게 영향을 주지 않는다. 본 논문에서 제안한 메커니즘은 로밍에 필요한 사용자와 WISP간의 인증을 수행할 수 있게 하였다. 그러나 과금에 관한 문제는 WISP간의 협약을 통해 이루어질 수 있으므로 향후에 WISP간의 과금 문제를 해결할 수 있는 연구를 수행할 것이다.

참고문헌

[1] 박성수, 신용식, 이동학, "이동통신 사업자의 공중 무선 LAN 서비스 수용방안", 한국통신학회, Vol. 19, No.5, May. 2002

[2] P. Calhoun, C. Perkins, "PPP EAP TLS Authentication Protocol", IETF RFC 2794, Mar. 2000.

[3] Byung-Rae Lee, Kyung-Ah Chang, Tai-Yun Kim, "Temporary Mobile User Certificate for Mobile Information Services in UMTS", IEICE TRANS. COMMUN. Vol.E83-B, No.8, 2000

[4] Gunter Horn, Bart Preneel, "Authentication and Payment in Future Mobile Systems", ESORICS, LNCS 1485, pp.277-293, 1998.

[5] B. Aboba, M. Beadles, "The Network Access Identifier", IETF RFC 2486, Jan. 1999

[6] VeriSign, "Secure Global Roaming for 802.11 WLANs", Technical Whitepaper, VeriSign Inc. 2002